ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

Modeling Secure XML Data Warehouses

Vijay Ramnath Sonawane[1], Snehal Subhash Patil[2], Punam Sharad Ratnaparkhi[3]

Assistant Professor, Dept. of IT, AVCOE, Sangamner, Maharashtra, India[1]

Student of M. E. (IT), AVCOE Sangamner, Maharashtra, India[2]

Student of M. E. (IT), AVCOE Sangamner, Maharashtra, India[3]

Abstract*:* Dataware houses are most ordinarily employed in strategic decision making processes. These systems integrate heterogeneous causes which are not only restricted to their interior enterprise facts & figures but also encompass facts & figures from the WWW, the last mentioned of which have become increasingly more significant in the conclusion making method in recent years. This gives motivation to use XML extensively in implementation of data warehouses. XML facilitates data and metadata interchange in between multiple heterogeneous data sources from the web and the data ware houses. Data ware houses may contain very high sensitive information, which needs to be protected. Securing the high sensitive information is the biggest challenge in the design of data ware houses. Despite of Implementation of data warehouses Technology is used.
In order to get rid of security issues, we have proposed a methodological approach for the model driven development of secure XML data warehouses.

Keywords: Secure XML Data Warehouse, Model Driven Development, MDA, XML, OLAP.

I. INTRODUCTION

Data Warehouse (DW) systems provide a Multidimensional (MD) outlook of huge amount of historical data from heterogeneous operational sources, Therefore delivering useful and sensitive data which allows decision makers to improve business processes in enterprises. The MD paradigm structures data into facts & dimensions. A fact having the interesting measures (fact attributes) of a business process (sales, deliveries, etc.), whereas a dimension comprises the context for analyzing a fact (product, customer, time, etc.) by means of hierarchically coordinated dimension attributes. It also assists in the investigation of facts and figures in a better kind because complete data provides more details.
Traditional DW systems allow enterprise persons to come by helpful knowledge from their organization's data by means of a variety of technologies, such as OLAP (OnLine Analytical Processing) or data mining. although, in order to provide richer insights into the dynamics of today's enterprise, it is actually desired that the data interior the association be blended with data from the out-of-doors, thus complementing the company's interior facts and figures with value-adding information (e.g., retail prices of goods traded by competitors). Since the amount of facts and figures accessible on the World Wide Web has been growing rapidly over the last ten years, World Wide Web facts and figures verify to be more and more helpful for this purpose. The major problem with facts and figures from the World Wide Web is that they are rather heterogeneous and convoluted. To overcome such drawbacks, designers of DW schemes make use of this data by utilising XML technologies.

It is significant to note that the facts and figures accessible on the Web need specific security considerations which have been expressly tailored to these schemes in order to allow their particularities to be apprehended correctly. Regrettably, whereas security matters have been advised in the development of customary data warehouses, present research needs advances with which to consider security when the goal stage is founded on XML technology.

We also identify a set of transformation directions that are adept to automatically develop not only the corresponding XML structure of the facts and figures warehouse from protected conceptual facts and figures warehouse forms, but also the security directions specified inside the facts and figures warehouse XML structure, thus permitting both facets to be implemented simultaneously. We additionally introduce our protected XML Data ware development approach, in which the protected conceptual Data ware data model, the PIM, is changed into a protected XML Dataware, as a PSM, by applying a set of transformation directions.
The principal difficulty with data from the Web is that they are rather heterogeneous and convoluted. DW systems designers confront this problem by employing XML technologies in order to make use of this data On the one hand, World Wide Web warehousing values XML as a means to ameliorate the extraction and integration of heterogeneous

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

Web facts and figures in the DW. On the other hand, document warehousing needs XML to deal with unstructured data in Dataware systems. In both situations XML is used to implement the MD form underlying the DW by defining the corresponding conceive artifacts (facts, dimensions, measures, hierarchies and so on) in alignment to facilitate the interchange of facts and figures and metafacts and figures amidst heterogeneous data sources and the DW system. The design of XML DWs is thus a cornerstone when it is necessary to use World Wide Web data in the conclusion making method, a situation which is becoming more and more common. The definition of design approaches for XML DW, which offer methodological structures founded on the Model Driven Architecture (MDA), is necessary and is one of the most interesting trials for the future in the locality of DW development. Furthermore, every design issue should be considered in the development process of an XML DW. More expressly, one of the most important design issues is security, which has to conceive rated day, been amazingly overlooked throughout the development of XML DWs. Considering that the data managed by DWs is often highly perceptive, and occasionally mentions to personal facts and figures (protected by the law in most countries), DWs should be protected from unauthorized data accesses (whatever the implementation platform is). In fact, a key obligation underlying these lately evolved data management schemes is a demand for adequate security, along with fine-grained flexible authorization models and get access to control mechanisms(since Datawares deal mostly with read operations). thus, rather than considering security once the scheme has been completely built, we believe that security and privacy measures should be integrated into all layers of the DW design, from the early stages of its development as another relevant requirement, signifying that much more robust, protected and platform independent products will be produced. In alignment to develop protected XML DWs considering confidentiality issues in the entire development method, from an early development stage to the last implementation, our proposal has been aligned with an MDA (Model Driven Architecture) architecture in which security models are embedded in and scattered throughout the high level system models, which are changed until their final implementation according to the MDA strategy. MDA can be utilised for this purpose, since it shares some similarities with the traditional MD modeling methods:1)a conceptual design phase is conveyed out, whose output is an implementation-independent and expressive conceptual MD model for the DW (i.e. a Platform Independent Model, PIM), 2) a logical design phase aspires to get a technology-dependent model(i.e. a Platform Specific Model, PSM) from the previously defined conceptual MD model, and 3) this ordered form is then the cornerstone for the implementation of the DW. After presenting some related works in the following section, we will introduce the secure XML DW development approach. The PIM is the secure conceptual DW data model, which will be semi-automatically changed into a secure XML DW, as a PSM, applying a set of transformation rules summarized. And in the end of the paper we will put ahead our conclusions and present our future work.

II. RELATED WORK

Background and Related work is organized according to the following topics:

A. MD DW Modeling,
B. XML DW Modeling
C. Security Integration into the Design Process
D. Security and Access Control Models for DWs.

A. MD DW Modelling:

Multidimensional database technology has reached a long way since its inception more than 30 years before. It has lately begun to come to the mass market, with foremost vendors now delivering multidimensional engines along with their relational database offerings, often at no additional cost. Multi-dimensional technology has furthermore made significant gains in scalability and maturity. Multidimensional data model emerged for use when the objective is to analyze rather than to perform on-line transactions.

Multidimensional model is founded on three key concepts: Modeling business rules Cube and measures Dimensions Multidimensional database technology is a key component in the interactive analysis of large amounts of facts and figures for decision-making purposes. Multidimensional data model is introduced based on relational components. Dimensions are formed as dimension relation, Dialects alike to organised query dialect. They cannot heal all dimensions and assesses symmetrically the delineation of multidimensional schema recounts multiple levels along a dimension, and there is at least one key ascribe in each grade that is included in the keys of the star schema in RD systems. Multidimensional database endow end-users to pattern data in a multidimensional environment. This is genuine merchandise power,, as it provides for the fastest, most flexible method to procedure multidimensional demands.

Data excavation applications request to find out information by seeking semi-automatically for before unidentified patterns and connections in multidimensional data bases. OLAP programs enable analysts, managers, and executives to

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 4, April 2013

gain insight into the performance of an organization through fast access to a broad kinds of views of data organized to reflect the multidimensional nature of the enterprise data.

B. XML DW Modelling:

In this paper, we use the Model Driven Architecture (MDA) to define security in the MD modeling of XML DWs. We concretely define security specifications in the Conceptual MD Data Model (PIM), individually of the target logical MD model. This Secure Conceptual MD Data Model will be used as a beginning point and will be semi-automatically changed into a Secure XML DW as a logical model (PSM) by applying Model to Model (M2M) Transformations. Finally, a Model to Model (M2T) transformation will construct the cipher for the Secure XML DW. For the model driven development of a secure XML DW it is therefore absolutely vital to present the following tasks (see Figure 1):

At the PIM level, the secure MD data model is carried out without considering the chosen expertise, since this model is independent of the platform. This MD PIM is comprised through an extended UML class diagram for DWs which furthermore permits the specification of security constraints on the model. At the PSM level, the data logical design is performed, taking into account the selected target platform in which the DW will be constructed. In our case, XML technology will be used for the implementation of the DW in any defended commercial database management system.

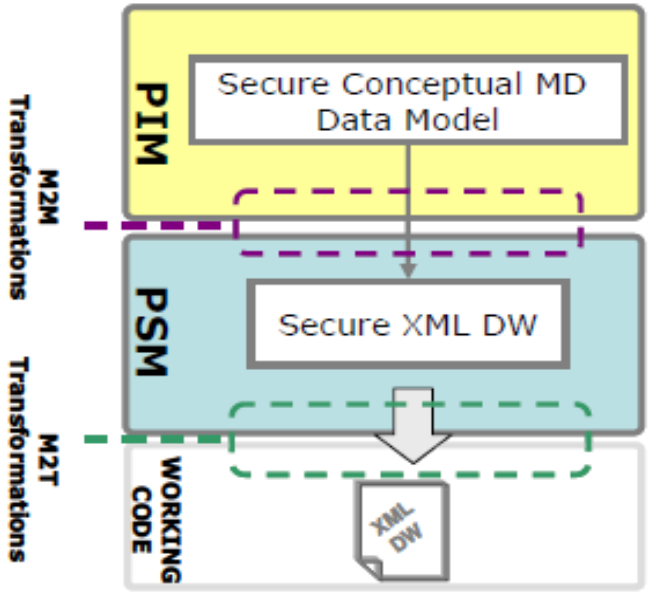

Fig. 1 Development approach for Secure XML DW

Security configuration:

Our Secure XML DB model (PSM) permits us to specify security compartments (SC), roles (SR) and levels (SL), whereas the most of XML database management systems use a role based security principle. Thus, the information concerning with the security configuration should be acclimatized from our PSM model to an RBAC policy. To obtain this purpose, each security compartment, role and level is implemented as a role with an identification name composed of a prefix ("SC", "SR" or "SL" depending of its source component) concatenated with the original title of the element in the PSM model. Then, each user must be added as a member of the roles that represent their privileges (security level, roles and compartments).

1. Definition of ACLs:

Once structural aspects and security roles have been specified, the security constraints defined should be constructed as ACLs which will be applied to the corresponding objects. We use an open policy where the access to all the assets of the DW is permitted, and then, we explicitly apply ACLs to refute certain resources to certain roles. In order to achieve this goal, we create an ACL for each role, in which the read privilege is denied. Finally, these ACLs will be applied depending on the security constraints defined.

2. Applying ACLs:
Firstly, an ACL provided by Oracle XML DB ("ro_all_acl.xml") is applied to grant read privileges to all roles. Then, based on the security privileges required to access each asset of the DW (facts, dimensions, bases and attributes) ACLs are applied to refute unauthorized accesses to each component. This information is defined in the PSM model associated with the resource by using a security information element composed of the level, roles and compartments which are required to access the resource.

C. Security integration into the design process:
Some relevant works can be found which concern a entire secure development but which focus on information systems in general. For example, UMLSec values UML to define and evaluate security specifications using formal semantics. Furthermore, Model Driven Security (MDS) uses the MDA approach to encompass security properties in high-level system models and to automatically develop secure system architectures. Inside the context of MDS, Secure UML is proposed as an extension of UML for modeling a generalized role based access control. On the other hand, Mokum is an active object oriented knowledge groundwork system for modeling, which permits the specification of security and integrity constraints and self-acting cipher generation. These are relevant contributions towards secure data systems development but are not specifically concentrated on DWs.

D. Security and access control models for DWs:
Since final users work with an MD model when querying a DW (facts, dimensions, classification hierarchies, etc.), security constraints must be characterised in periods of MD modeling. There are some intriguing plans for the addition of security in Dataware houses, but they are not conceived for including into MD modeling as part of the DW design method, and, inconsistent security measures may consequently be characterised. Katic et al. present a security model founded on metadata to define user groups and views. Rosenthal and Sciore integrate security from the data sources and propagate it to DW design. Other proposals define authorization models and security for DWs but they deal solely with OLAP operations (such us roll-up or drill-down).

III. CONCLUSIONS AND FUTURE WORKS

In this work we have proposed an approach for the model driven development of Secure XML Dataware house. Our approach starts by defining the protected conceptual MD model (PIM) represented by means of the secured UML profile called SECDW, independently of the target logical MD model. This PIM is used as a beginning point and is then semi-automatically changed into a secure XML Dataware, as a logical model (PSM), by applying Model to Model (M2M) Transformations. Here, we have specified these transformation directions with which to automatically populate not only the corresponding XML structure of the Dataware from the secure conceptual models of the DW, but furthermore the security directions specified within the DW XML structure, thus permitting both aspects to be constructed simultaneously. We are now working on several different lines, in an attempt to extend the proposal presented in this paper. Moreover, we are furthermore working on the automation of the transformations between the meta models and the corresponding models using the Query View Transformation (QVT) proposal. A further goal is that of performing several case studies to detect new desires. These would furthermore analyze the benefits of incorporating security facets supplied by the distinct XML DB administrators, and not only those which are native. The next step will be to encompass our proposal in the case tool that we are evolving for the semiautomatic development of Secure XML DW.

REFERENCES

[1] Abelló, A., J. Samos, and Saltor, F. YAM2: a multidimensional conceptual model extending UML. Information Systems. 31(6): p. 668-677, 2006.

[2] Beyer, K.S., et al., Extending XQuery for Analytics. In:ACM SIGMOD Int. Conference on Management of Data. 2005: Baltimore, Maryland. p. 503-514.

[3] Basin, D., J. Doser, and Lodderstedt, T. Model Driven Security: from UML Models to Access Control Infrastructures. ACM Transactions on Software Engineering and Methodology. 15(1): p. 39-91, 2006.

[4] Binh, N.T., Tjoa, A.M. and Wagner, R. An object oriented multidimensional data model for OLAP, in Web-Age Information Management. 2000. p. 69-82.

[5] Abelló, A., J. Samos, and Saltor, F. A Framework for the Classification and Description of Multidimensional DataModels. In: 12th Int. Conference on Database and Expert Systems Applications (DEXA'01). LNCS 2113: p. 668-677, 2001.

[6] Golfarelli, M., S. Rizzi, and Vrdoljak, B.Data Warehouse Design from XML Sources. DOLAP 2001.

[7] Priebe, T. and G. Pernul. Towards OLAP Security Design - Survey and Research Issues. In DOLAP'00. 2000. Washington DC, USA.

[8] Tryfona, N., F. Busborg, and Christiansen, J. starER: A Conceptual Model for Data Warehouse Design. In: ACM 2nd International Workshop on Data Warehousing and OLAP (DOLAP'99). 1999. Missouri, USA: ACM.

[9] Mouratidis, H. and P. Giorgini, Integrating Security and Software Engineering: Advances and Future Vision. IGI Global. 2006.

[10] Katic, N., Quirchmay, G., Schiefer, J., Stolba, M. and Tjoa, A.M. A Prototype Model for Data Warehouse Security Based on Metadata. In 9th Int. Workshop on Database and Expert Systems Applications DEXA'98. 1998. Vienna, Austria.: IEEE Computer Society.

BIOGRAPHY

Mr. Sonawane Vijay Ramnath completed his B.E in IT from North Maharashtra University and M.E in Computer Science and Technology from Shivaji University.

Mr. Patil Snehal Subhash Completed his B.E. in information Technology from University of Mumbai in 2010. He is currently doing his M.E. in Information Technology from University of Pune.

Ms. Ratnaparkhi Punam Sharad has completed B.E. in information Technology from MET, BKC, Nashik ,University of pune in 2011. She is working as a lecturer in Matoshri college of engineering and research centre. Nashik , she is currently doing her M.E. in Information Technology from University of Pune.